

Fig. 1

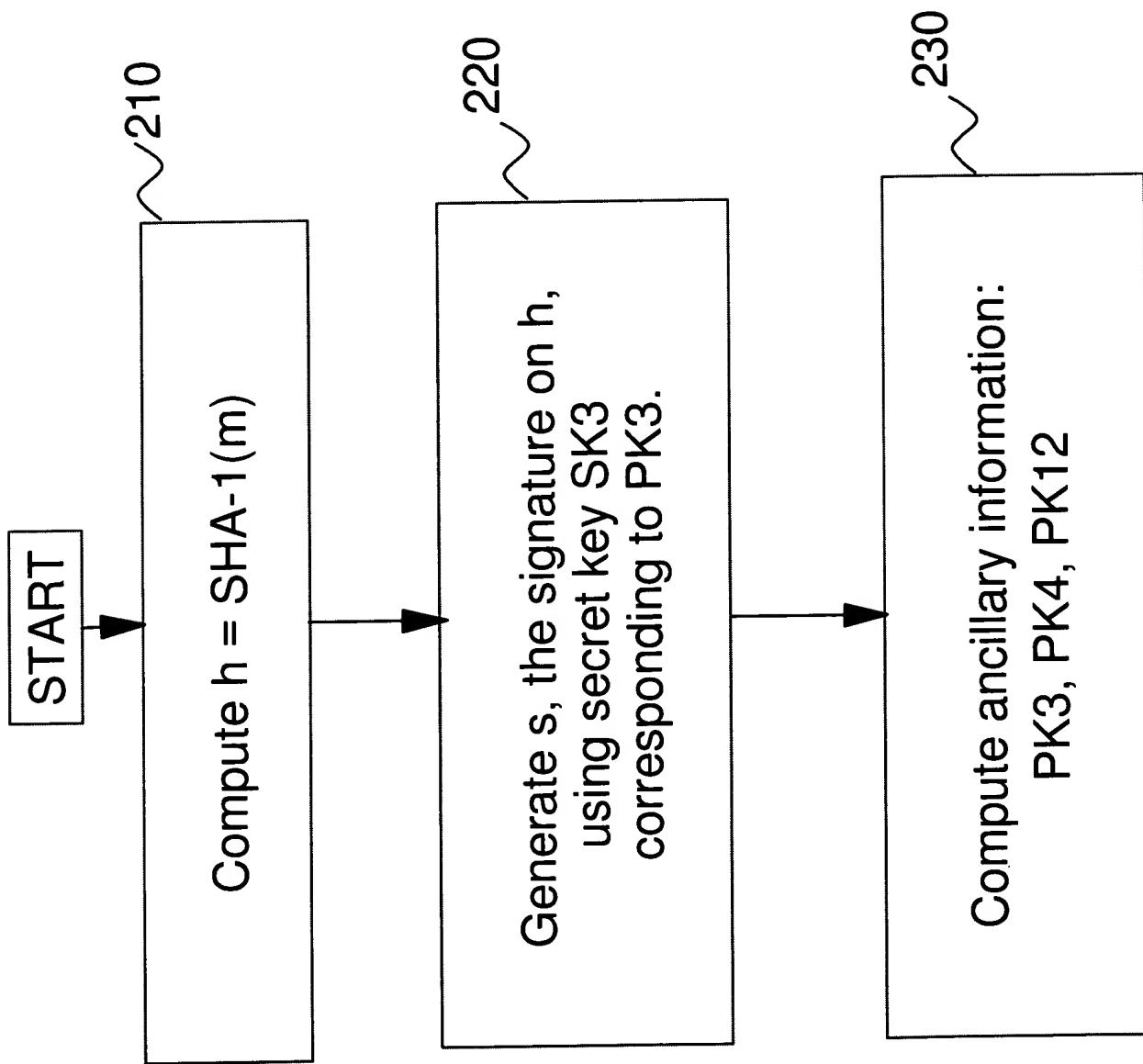


Fig. 2.

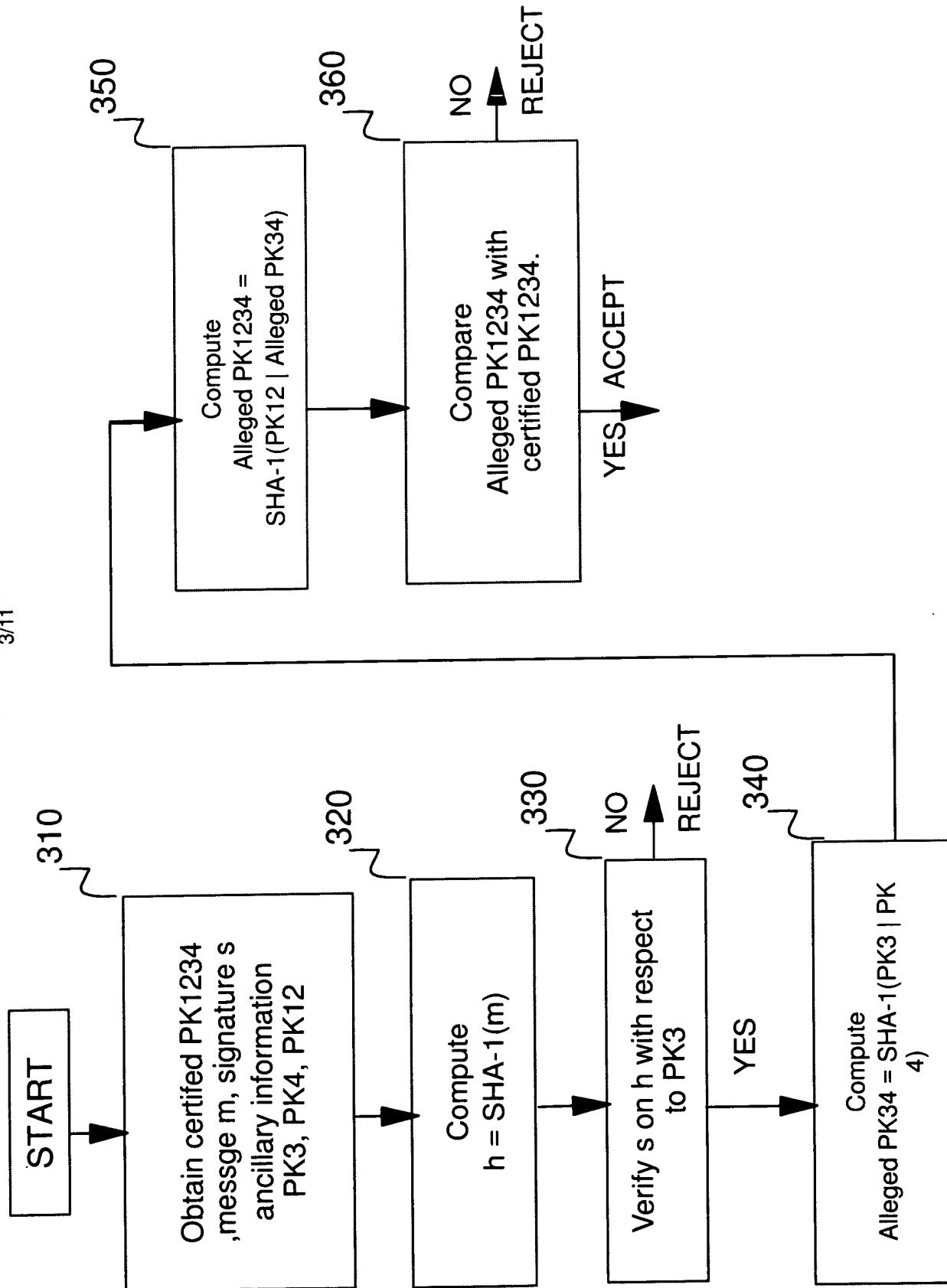


Fig. 3.

START

Choose g_1, g_2, g_3
uniformly at random

Define $g(x) =$
 $G(g_1, x)$

Compute 36 1-time
keys as in Fig. 5.
Let PK_1, \dots, PK_{36}
be the generated
1-time public keys.

Form PK_{36} , the
36 time public key
as in Fig. 6.

Fig. 4 .

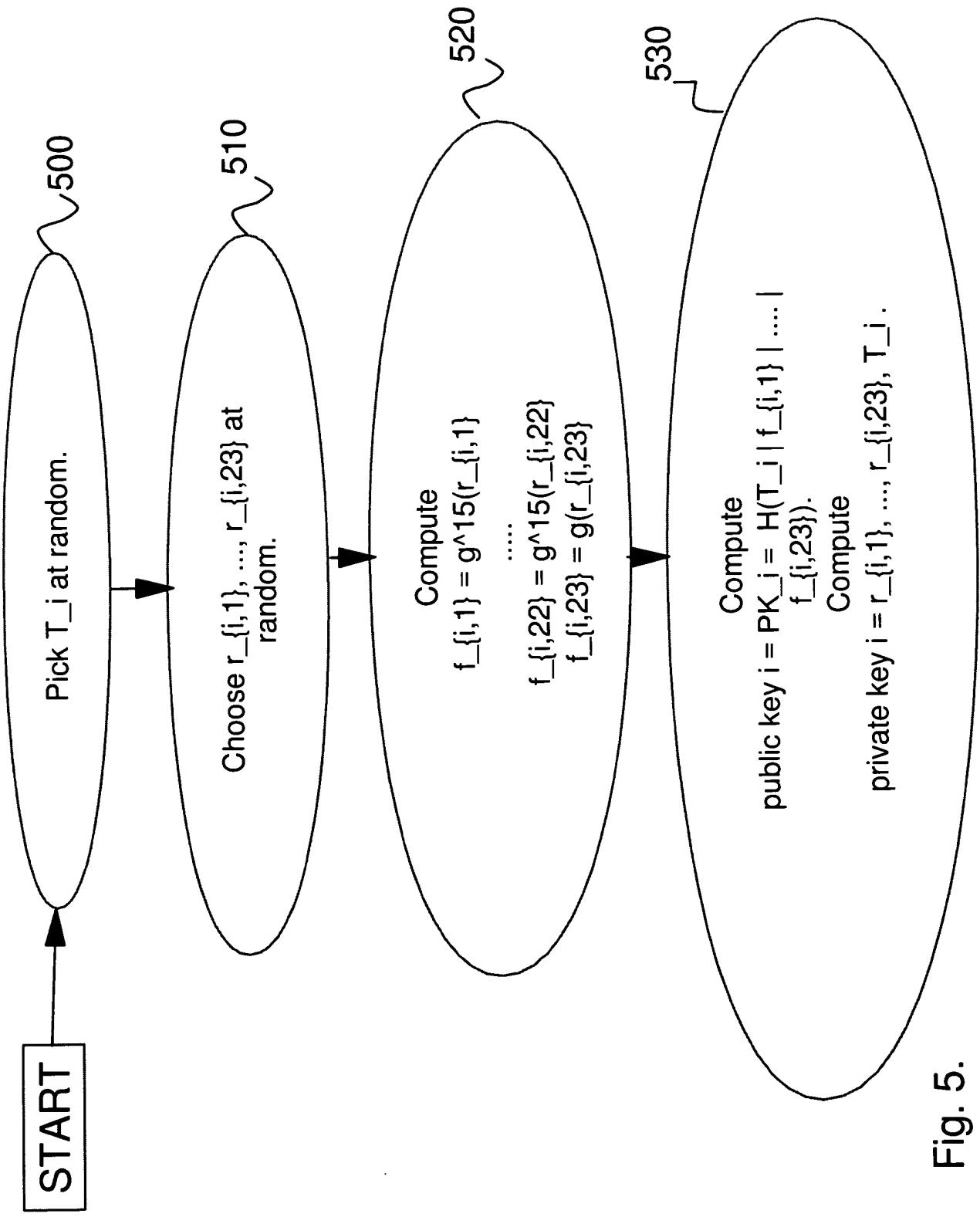


Fig. 5.

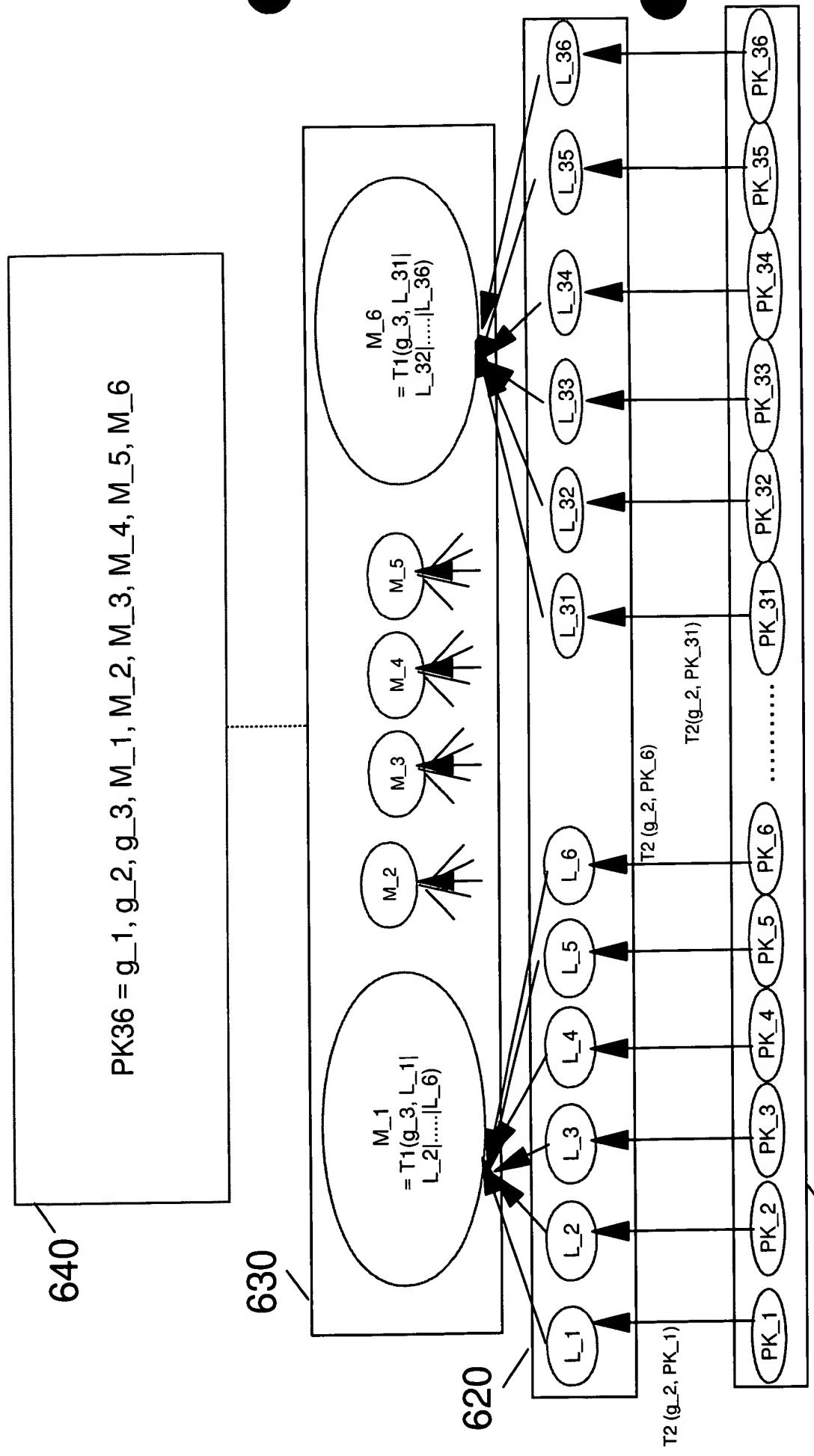


Fig. 6

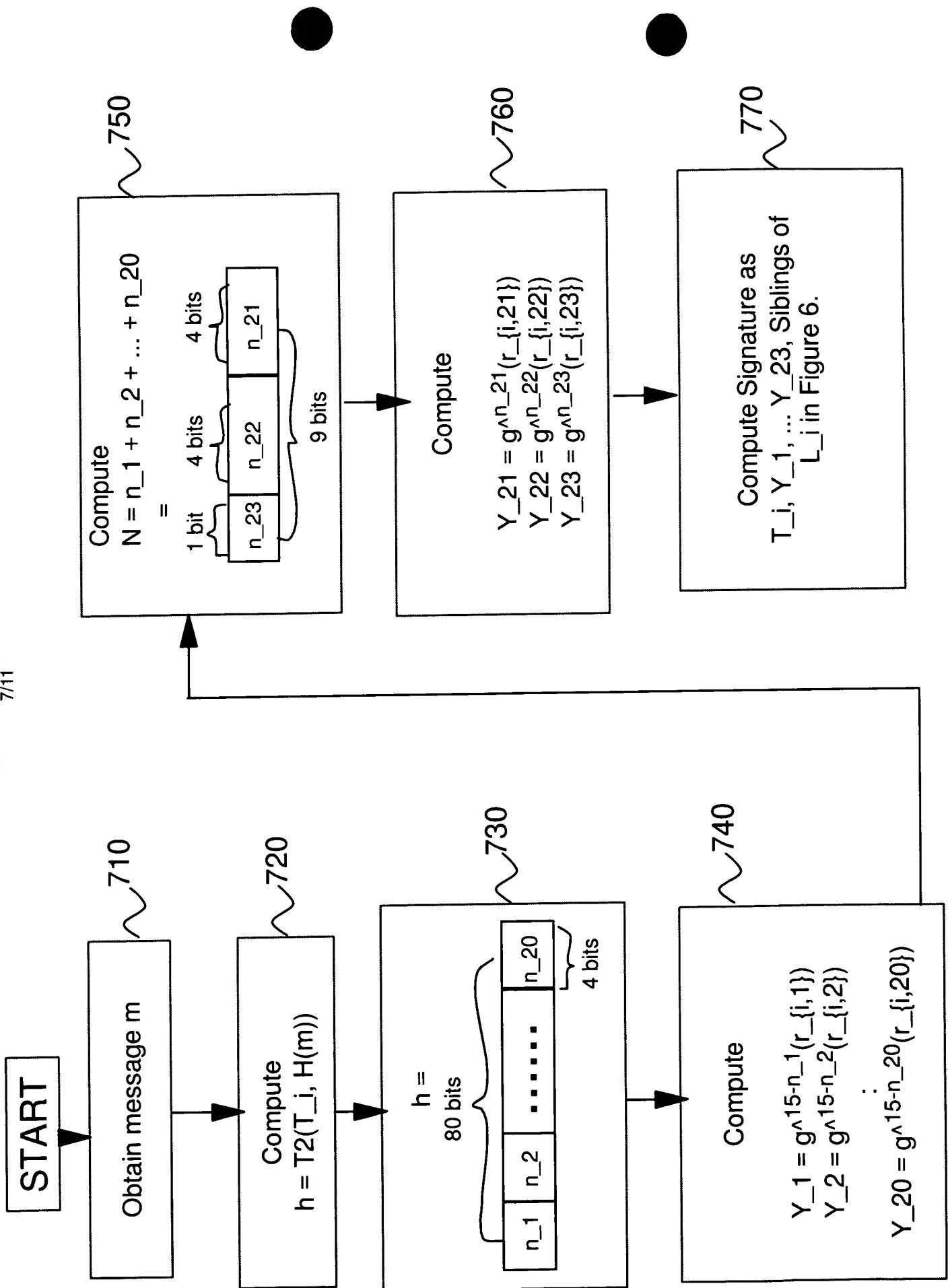


Fig. 7.

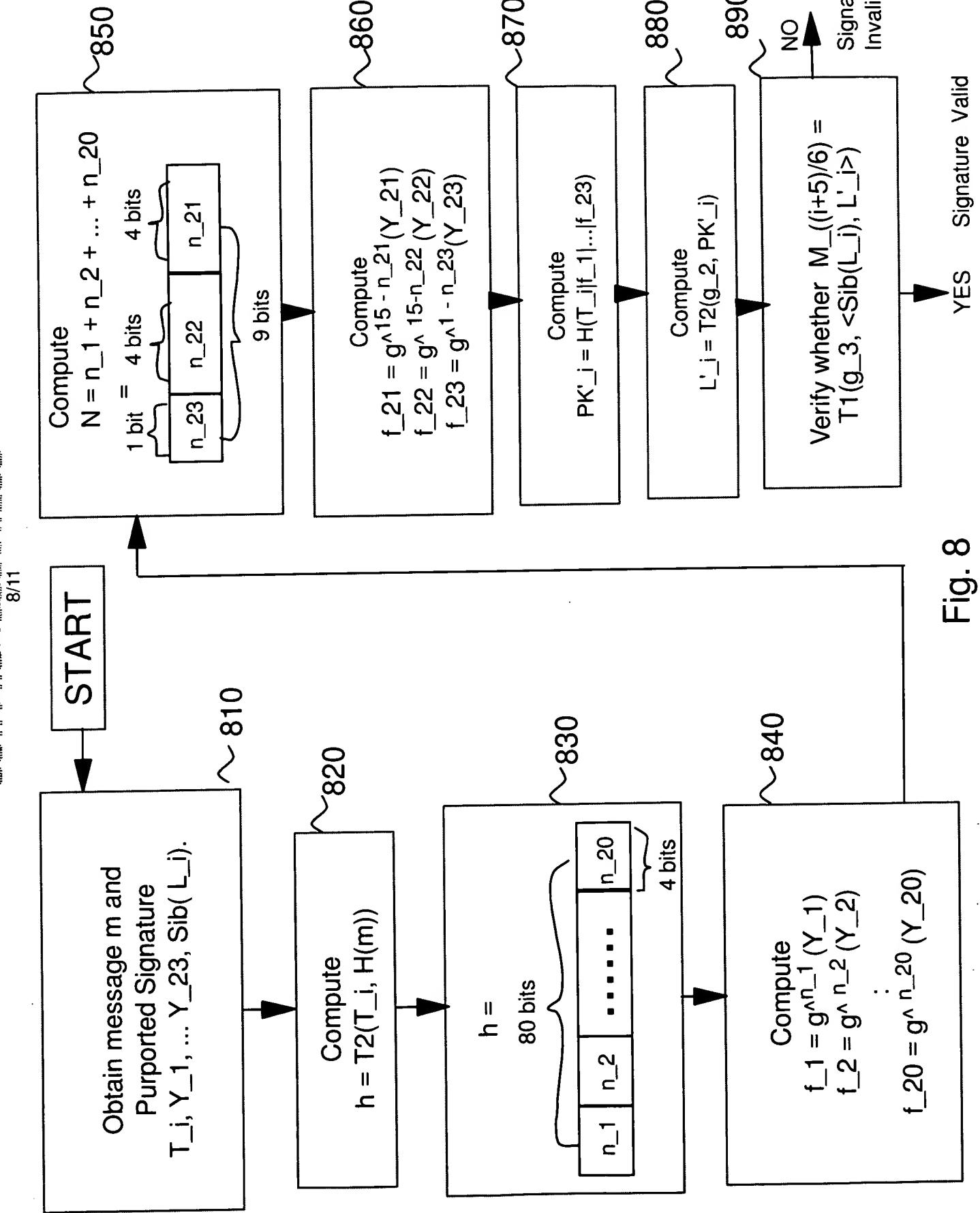


Fig. 8

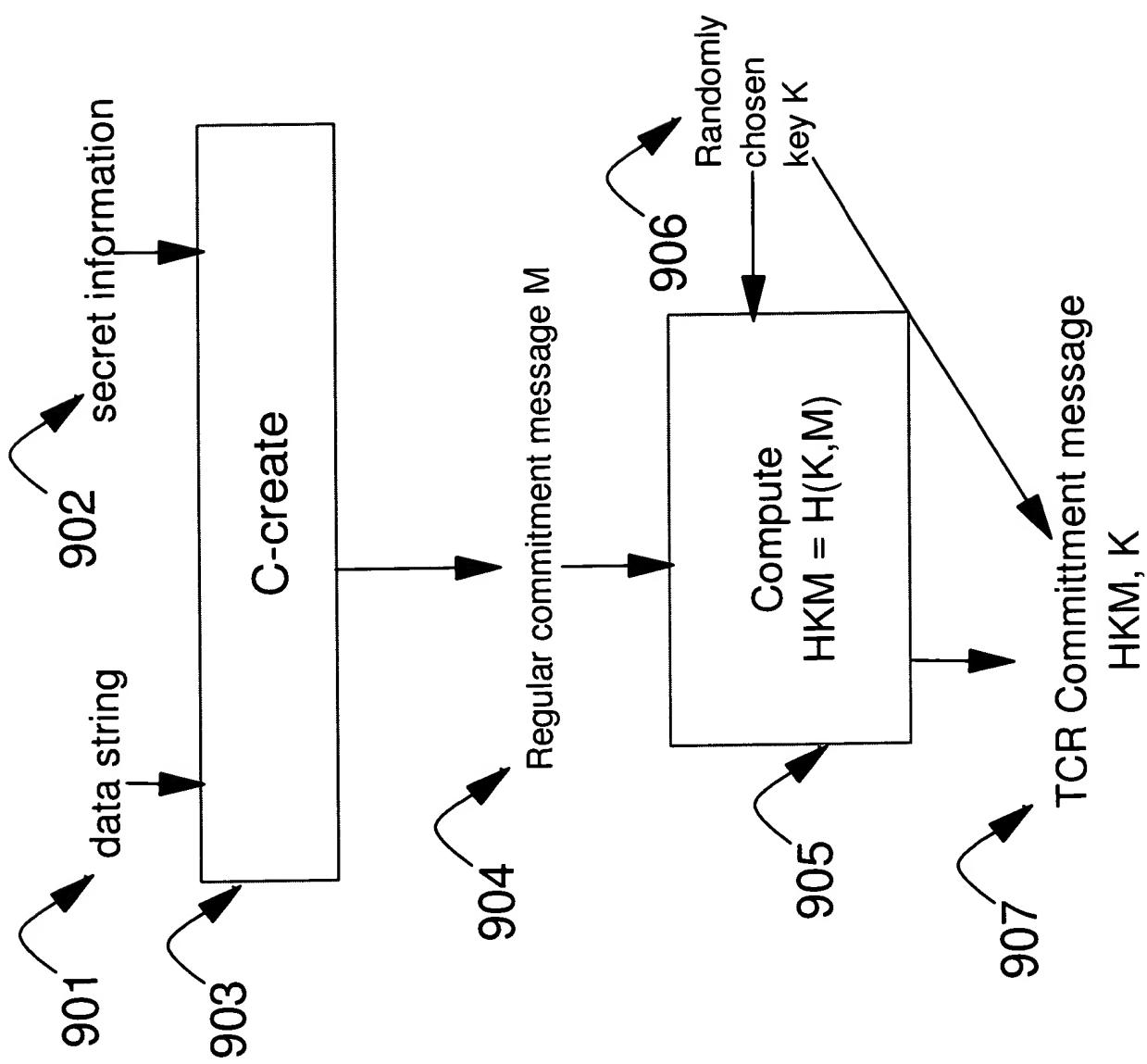


Fig. 9

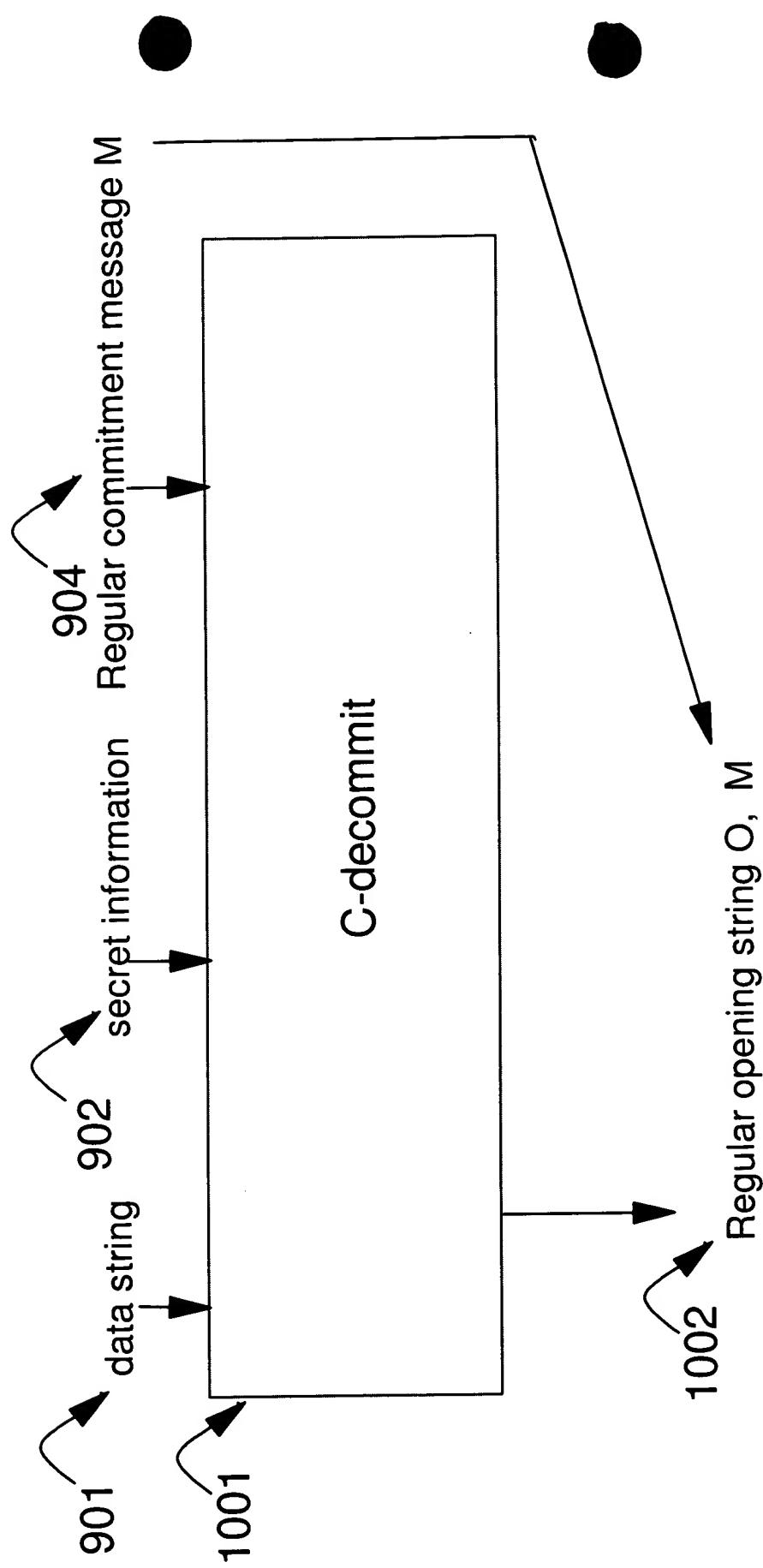


Fig. 10

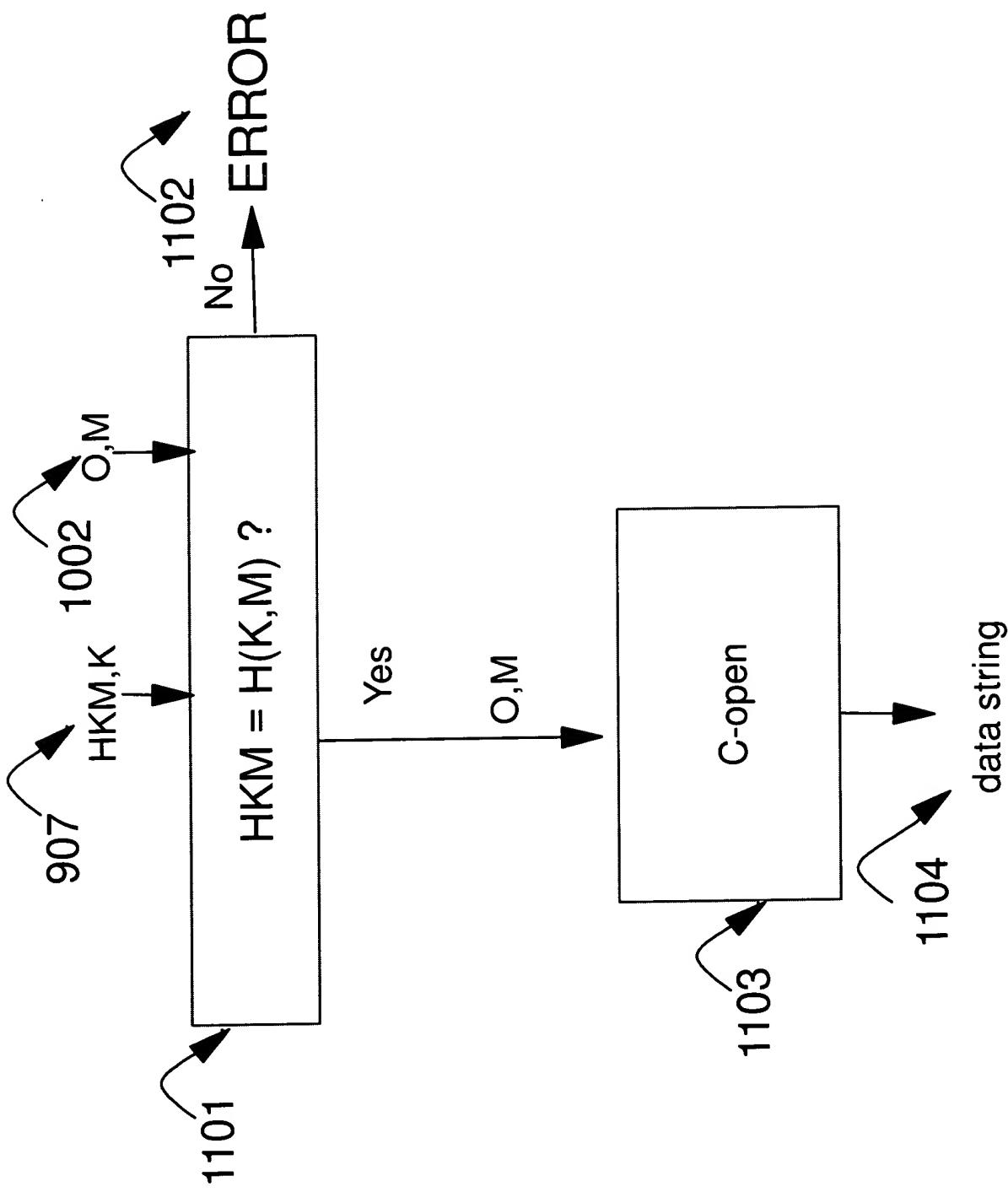


Fig. 11